IN THE CLAIMS:

1.   (Original) A method in a data processing system for reporting security situations, comprising the steps of:

    logging events by storing event attributes as an event set, wherein each event set includes
        a source attribute, a target attribute and an event category attribute;

    classifying events as groups by aggregating events with at least one attribute within the
        event set as an identical value;

    calculating severity levels for the groups;

    calculating delta severities from the severity levels; and

    propagating the delta severities to a higher-level correlation server.

2.   (Original) The method of claim 1, wherein the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups.

3.   (Original) The method of claim 1, wherein the events include at least one of a web server event, an electronic mail event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation.

4.   (Original) The method of claim 1, further comprising:

    calculating the threshold value based on at least one of the source attribute of the event
        sets within the group, the target attribute of the event sets within the group, the
        event category attribute in each event set of the group, and the number of
        attributes in each event set of the group that are held constant across all of the
        event sets in the group.

5.   (Original) The method of claim 1, wherein the target attribute represents one of a computer and a collection of computers.

6.   (Original) The method of claim 1, wherein the source attribute represents one of a computer and a collection of computers.

7.   (Original) The method of claim 1, further comprising:
aggregating a subset of the groups into a combined group.

8.   (Withdrawn) A method, in a data processing system, of establishing a severity level for multiple groups of computers, comprising:
        receiving a plurality of delta severity levels;
        performing a first mathematical operation on the plurality of delta severity levels to form
                a new delta severity level;
        if the data processing system is the top level of a hierarchy of servers, performing a
                second mathematical operation on the new delta severity level and a stored
                severity level to form a new severity level; and
        if the data processing system is not the top level of a hierarchy of servers, propagating the
                new delta severity level to a higher-level correlation server.

9.   (Withdrawn) The method of claim 8, wherein the first mathematical operation is one of addition, arithmetic mean, and geometric mean.

10.   (Withdrawn) The method of claim 8, wherein the second mathematical operation is one of addition, arithmetic mean, and geometric mean.

11.   (Original) A computer program product in a computer readable medium for reporting security events, comprising instructions for:
        logging events by storing event attributes as an event set, wherein each event set includes
                a source attribute, a target attribute and an event category attribute;
        classifying events as groups by aggregating events with at least one attribute within the
                event set as an identical value;
        calculating severity levels for the groups;
        calculating delta severities from the severity levels; and

Page 3 of 11
Black et al. – 09/942,633

propagating the delta severities to a higher-level correlation server.

12.   (Original) The computer program product of claim 11, wherein the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups.

13.   (Original) The computer program product of claim 11, wherein the events include at least one of a web server event, an electronic mail event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation.

14.   (Original) The computer program product of claim 11, comprising additional instructions for:

    calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group.

15.   (Original) The computer program product of claim 11, wherein the target attribute represents one of a computer and a collection of computers.

16.   (Original) The computer program product of claim 11, wherein the source attribute represents one of a computer and a collection of computers.

17.   (Original) The computer program product of claim 11, comprising additional instructions for:

    aggregating a subset of the groups into a combined group.

18.   (Withdrawn) A computer program product in a computer readable medium, containing instruction code operable in a data processing system, said computer program product comprising instructions for:

receiving a plurality of delta severity levels;

performing a first mathematical operation on the plurality of delta severity levels to form a new delta severity level;

if the data processing system is the top level of a hierarchy of servers, performing a second mathematical operation on the new delta severity level and a stored severity level to form a new severity level; and

if the data processing system is not the top level of a hierarchy of servers, propagating the new delta severity level to a higher-level correlation server.

19.   (Withdrawn) The computer program product of claim 18, wherein the first mathematical operation is one of addition, arithmetic mean, and geometric mean.

20.   (Withdrawn) The computer program product of claim 18, wherein the second mathematical operation is one of addition, arithmetic mean, and geometric mean.

21.   (Original) A data processing system for reporting security events, comprising:

a bus system;

a memory;

a processing unit, wherein the processing unit includes at least one processor; and

a set of instructions within the memory,

wherein the processing unit executes the set of instructions to perform the acts of:

logging events by storing event attributes as an event set, wherein each event set includes a source attribute, a target attribute and an event category attribute;

classifying events as groups by aggregating events with at least one attribute within the event set as an identical value;

calculating severity levels for the groups;

calculating delta severities from the severity levels; and

Page 5 of 11
Black et al. – 09/942,633

propagating the delta severities to a higher-level correlation server.

22.   (Original) The data processing system of claim 21, wherein the severity levels are calculated based on at least one of the number of event sets within each of the groups, the source attribute of the event sets within each of the groups, the target attribute of the event sets within each of the groups, and the event category attribute of the event sets within each of the groups.

23.   (Original) The data processing system of claim 21, wherein the events include at least one of a web server event, an electronic mail event, a Trojan horse, denial of service, a virus, a network event, an authentication failure, and an access violation.

24.   (Original) The data processing system of claim 21, wherein the processing unit executes the set of instructions to perform the act of:

calculating the threshold value based on at least one of the source attribute of the event sets within the group, the target attribute of the event sets within the group, the event category attribute in each event set of the group, and the number of attributes in each event set of the group that are held constant across all of the event sets in the group.

25.   (Original) The data processing system of claim 21, wherein the target attribute represents one of a computer and a collection of computers.

26.   (Original) The data processing system of claim 21, wherein the source attribute represents one of a computer and a collection of computers.

27.   (Original) The data processing system of claim 21, wherein the processing unit executes the set of instructions to perform the act of:

aggregating a subset of the groups into a combined group.

28.   (Withdrawn) A data processing system for reporting security events, comprising:
a bus system;

a memory;

a processing unit, wherein the processing unit includes at least one processor; and

a set of instructions within the memory,

wherein the processing unit executes the set of instructions to perform the acts of:

> receiving a plurality of delta severity levels;

> performing a first mathematical operation on the plurality of delta severity levels
>> to form a new delta severity level;

> if the data processing system is the top level of a hierarchy of servers, performing
>> a second mathematical operation on the new delta severity level and a
>> stored severity level to form a new severity level; and

> if the data processing system is not the top level of a hierarchy of servers,
>> propagating the new delta severity level to a higher-level correlation
>> server.

29.   (Withdrawn) The computer program product of claim 28, wherein the first mathematical operation is one of addition, arithmetic mean, and geometric mean.

30.   (Withdrawn) The computer program product of claim 28, wherein the second mathematical operation is one of addition, arithmetic mean, and geometric mean.

Page 7 of 11
Black et al. – 09/942,633